The official voice of the Air Force Research Laboratory
news@afrl
Roundups
June 2001

$8.4M contract aimed at curbing computer attacks

by Fran Crumb, Information Directorate

ROME, N.Y. — The Air Force Research Laboratory (AFRL) Information Directorate has awarded an $8,444,092 contract to Orincon Corp. of San Diego, Calif., for research to enhance detection of attacks on computer systems.

Under terms of the 10-month agreement, "Coordinated Distributed Attack Detection (CDAD)," Orincon researchers will develop capabilities to monitor network traffic in real-time — alerting analysts about information attacks and providing recommendations for information-based countermeasures.

"The CDAD program will develop technology to be called Distributed Agent Information Watch (DAIWatch)," said Robert J. Vaeth, program manager in the directorate's Information Grid Division. "DAIWatch will be based on sensor agents that can detect a broad set of events and intelligent agents that can fuse events into activities and reason about activities within real-time context to relate them to attacks."

Software agents have their own internal problem-solving abilities, which allow them to continuously collect specific information and determine when new information must be obtained to remain current in support of decision-makers. Agent technology has the potential to assist users with the informational changes and uncertainty associated with strategy and tactics for defensive information warfare.

"The DAIWatch system is dynamically scalable and reconfigurable, which allows it to adapt to changing circumstances in the task environment and dynamically add capabilities," said Vaeth. "Most importantly, the system has been designed and implemented to maximize the rate of true detections while minimizing false alarms."

Lori L. Smith of the directorate's Contracting Division negotiated the Orincon agreement. **@**